National Aeronautics Space Administration

NASA Safety Center
Suzanne Otero

ARES Corporation
Philip Mongan

Using Case Studies To Assure
MISSION SUCCESS

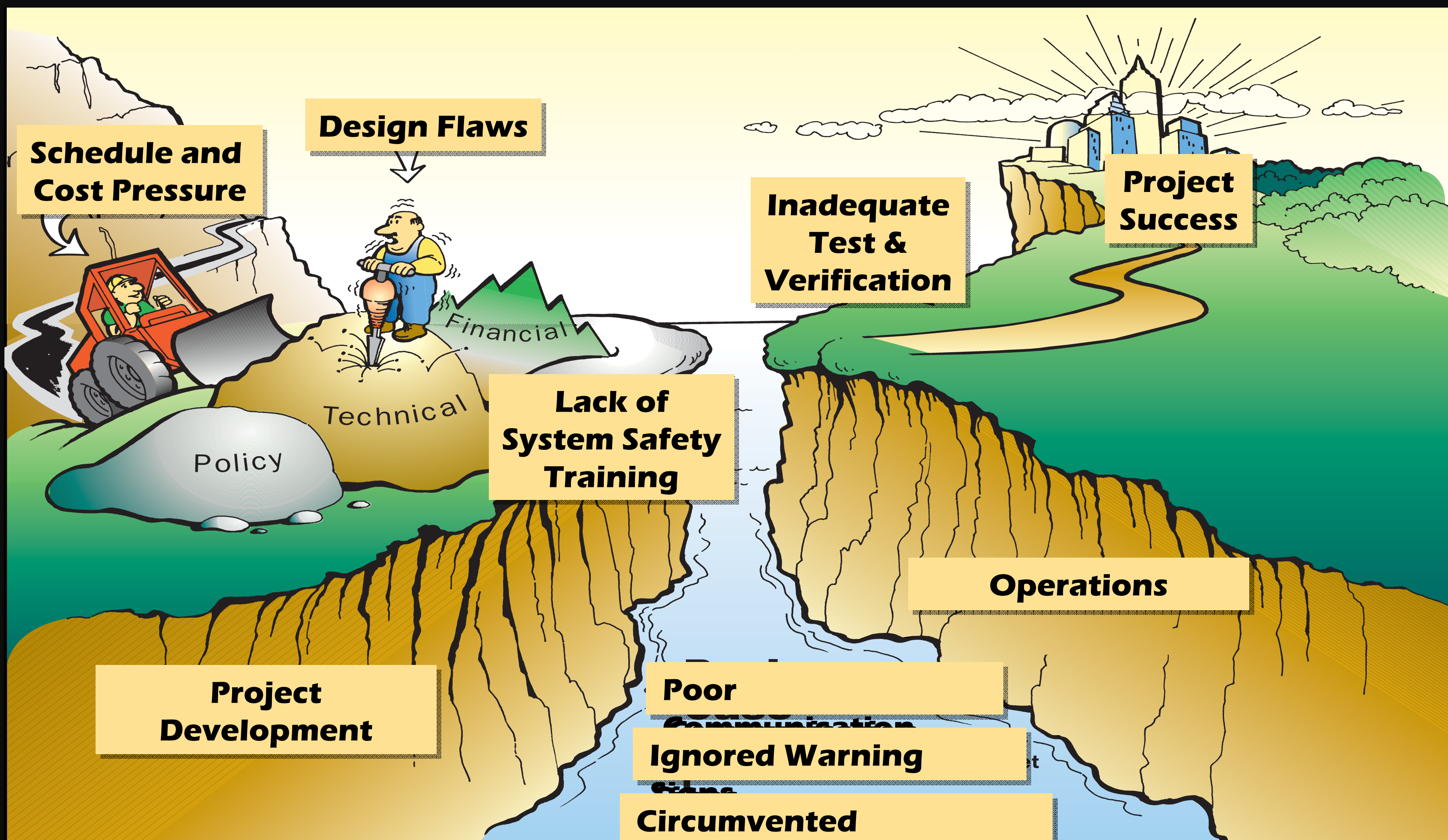
NASA SAFETY CENTER

Purpose of This Session

Introduce you to…

- The value of case study based discussion within your project teams
- How these case studies can be used to create well integrated and effective project teams
- Two different types of case studies that you can easily access via web
- Structured training and seminars that you can schedule for your program

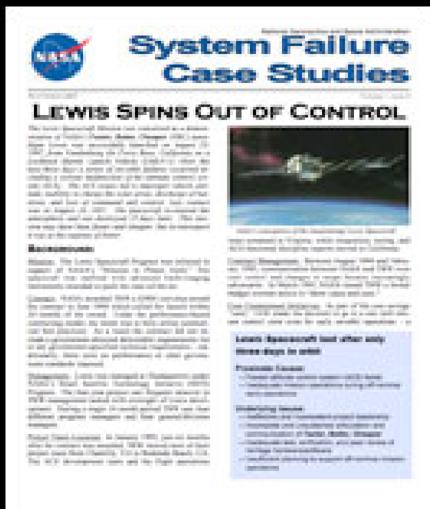
Projects Can Be A Treacherous Journey



Why Case Studies Are So Effective

- They use a storytelling approach to describe interesting events or mishaps
- They engage the reader into the thought processes and emotions of those that lived the experience
- They enlighten us to the ways in which scenarios could unfold, and what we can each do to disrupt an undesired outcome

An Intro To Two Types Of Case Studies



System Failure Case Studies

LEWIS SPINS OUT OF CONTROL

- ***System Failure Case Studies*** - focusing on larger scale more complex and “highly visible” events which have occurred both inside and outside of NASA

National Aeronautics and Space Administration

NASA SAFETY CENTER CASE OF INTEREST

Ghost in the Machine

RF-Controlled Crane Safety

Primary Case

- ***Cases of Interest*** - focusing on cases which have high risk/mishap potential

System Failure Case Studies
(SFCS)

Common Mishap Themes

- A study of 13 case studies identified common mishap themes

Lack of System Safety Awareness or Training | Engineering Design Flaws | Improper or Circumvented Procedures (Configuration Management) | Inadequate Verification and Testing | Ignored "Warning Signs" | Poor Communication | Schedule and/or Cost Pressures | Human Interaction with System | Ineffective Program/Project Management | Automated System Failure | Developing New Technologies

	Lack of System Safety Awareness or Training	Engineering Design Flaws	Improper or Circumvented Procedures (Configuration Management)	Inadequate Verification and Testing	Ignored "Warning Signs"	Poor Communication	Schedule and/or Cost Pressures	Human Interaction with System	Ineffective Program/Project Management	Automated System Failure	Developing New Technologies
2006											
Death on the Steppes	X	X	X		X		X		X	X	X
Submarine Down	X	X		X				X			
2007											
Almost Perfect	X	X	X			X			X	X	
Derailed	X	X	X	X	X			X			
Innovations Pushed Too Far Too Fast	X	X		X	X	X	X				X
Lewis Spins Out of Control	X	X	X	X	X	X	X	X	X	X	
Rocky Mountatin Death Trap	X	X	X	X				X	X		
Supercritical	X	X	X	X	X		X	X	X		X
2008											
Fire in the Cockpit	X	X		X	X		X				
Forrestal in Flames	X	X	X	X	X	X	X		X	X	
Powerless	X	X	X	X		X				X	
Refinery Ablaze - 15 Dead	X	X	X		X		X	X	X	X	
Two Rods Don't Make It Right	X	X	X		X	X	X	X	X		

NSC NASA SAFETY CENTER

System Failure Case Studies (SFCS)

THAT SINKING FEELING

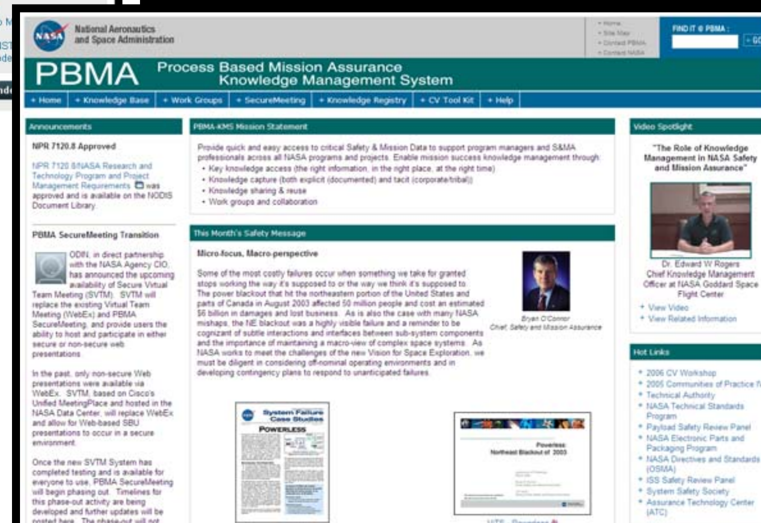
"The project successfully rejected … prescriptive engineering, onerous quality requirements, and outdated concepts of inspection …"

A Petrobras executive after delivering superior financials

SFCS History

- System Failure Case Studies (SFCS)
- Began in 2006
- Produced monthly
- Mix of NASA and non-NASA case studies
- 4 page write-up complimented by PowerPoint brief with highlights
- Key Points
  - Background and overview of failure
  - Proximate and underlying causes
  - Applicability to NASA

SFCS – Where To Find



Internal to NASA
http://nsc.nasa.gov
or
External to NASA
http://pbma.nasa.gov

SFCS Archive

Title	ViTS	SFCS	Video
Powerless - Northeast Blackout of 2003			
Fire in the Cockpit - The Apollo 1 Tragedy			
Forrestal In Flames - US Aircraft Carrier Forrestal			
Lewis Spins Out of Control - Lewis Space Craft			
Supercritical - SL-1 Nuclear Reactor			
Almost Perfect - X31 (Videos are NASA Only)			
Rocky Mountain Death Trap: The Mann Gulch Fire - Team Dynamics			
Innovation Pushed Too Far Too Fast - R-101 Dirigible			
Derailed - The Eschede Train Disaster			
Close Call - Location: VAB, KSC - Harness Safety			
Atlas Centaur (AC-67) Lightning Strike Mishap 1987			
Radiation Cancer Therapy Machine Mishaps in 1985-86 due to Safety Critical Software Control Errors - Radiation Therapy Overdose			
Mishap at an Explosives R&D Laboratory - ATK Thiokol Explosives Lab			
Ames Arc Jet DC Power Supply Fire			
The Davis-Besse Close Call - Davis-Besse Nuclear Reactor			
Air Force Atlas Mishap Due to Unintended Mixing of LOX and Hydrocarbons 1975 - Air Force Atlas 71F			
SUBSAFE - USS Thresher, SSN 593, Lesson Learned			
Are We Prepared for the Upcoming Hurricane Season?			
A Gift - STS-3			
Fatal Mishap Resulting from a Pressure System Operation in Government Laboratory			
Chemical Safety Board's (CSB) Findings in New York Chemical Waste-Mixing Incident - Kaltech Chemical			
And some have said "software isn't critical" - Ariane 5			
Chemical Safety Board's Preliminary Findings in BP Texas City Refinery Accident			
A Tale of Two Failures... the difference between a "Bad Day" and a "Nightmare" - Delta II 7925/Long March CZ-3B			
Death on the Steppes - The Nedelin Rocket Disaster			
Failures, Mishaps and Root Cause Analysis - Hurricane Katrina			
Steam Locomotive Firebox Explosion on the Gettysburg Railroad near Gardners, Pennsylvania			
Equilon Refinery Accident Anacortes, WA			
Bhopal: When Hazard Controls Aren't			
MGM Grand Hotel Fire Disaster, A Turning Point for Fire Protection Codes			

SFCS - Structured Training and Seminars

Training	Objectives	Forum	Time
Familiarization Brief	**- Introduce SFCS's**	**Auditorium or seminar**	**20-30 minutes**
Issue Brief	**- Focus on specific issue**	**Auditorium or seminar**	**20-30 minutes**
Case Study Analysis	**- Lessons learned - Increase awareness of current risks**	**Seminar/ Focused Group**	**1 hour to 1+30**
Knowledge Café (3 Case Studies)	**- Wide Breadth of lessons learned - Increase awareness of current risks**	**Seminar/ Focused Group**	**3 Hours**
Decision Making Seminar (1 Pre-failure Case Study)	**- In depth lessons learned - Increase awareness of current risks - Emphasis on risk identification and mitigation**	**Seminar/ Focused Group**	**4 Hours**

Cases of Interest
(CoI)

NPR 7150.5D para 6.2.1g:
"*Assure that the project team seeks to learn and apply relevant lessons* from successful flight systems and ground support projects, *mission anomalies and mishaps.*"

Why Cases of Interest?

Knowledge Capture and Dissemination to:

•Ensure that we're informed risk takers

•Manage the routine risks in the workplace effectively

•Preserve our resources for the execution of the NASA Mission.

- Given the current breadth of information contained in events that are not high visibility….
- How do we "tap" into these events and experiences
  - For audit planning?
  - For training/technical excellence?
  - For awareness? For targeted audiences?
  - ***For Mishap prevention and Mission Success?***

Type A's and B's-138

Type C's - 6,529

Type D's - 8,467

Type Close Calls - 23,164

*Data collected in IRIS between 1984 to 2007

What was needed was an approach to…

- Analyze the bulk of data utilizing filters to identify precursors and hazards
- Identify a case for storytelling and distribution that will emphasize the precursors and hazards
- Include suggestions for prevention, training, auditing
- “Brand” this information obtained from the analysis so it is recognizable and meets expected knowledge management needs

*Incident Reporting Information System

COI Prevention Marker analysis

- Could there have been a potentially catastrophic event associated with the IRIS case?
- Are broad effects likely?
- Are there serious consequences/effects across system boundaries? (coupled, uncoupled systems and or complex systems)
- Special Case-Is there a control failure?
- Are there hazardous latent conditions?
- Is there extensive incident documentation in the IRIS case file?
- Is there extensive corrective action documentation in the IRIS case file?
- Is there a time critical hazard or “top level risk” that needs to be addressed?

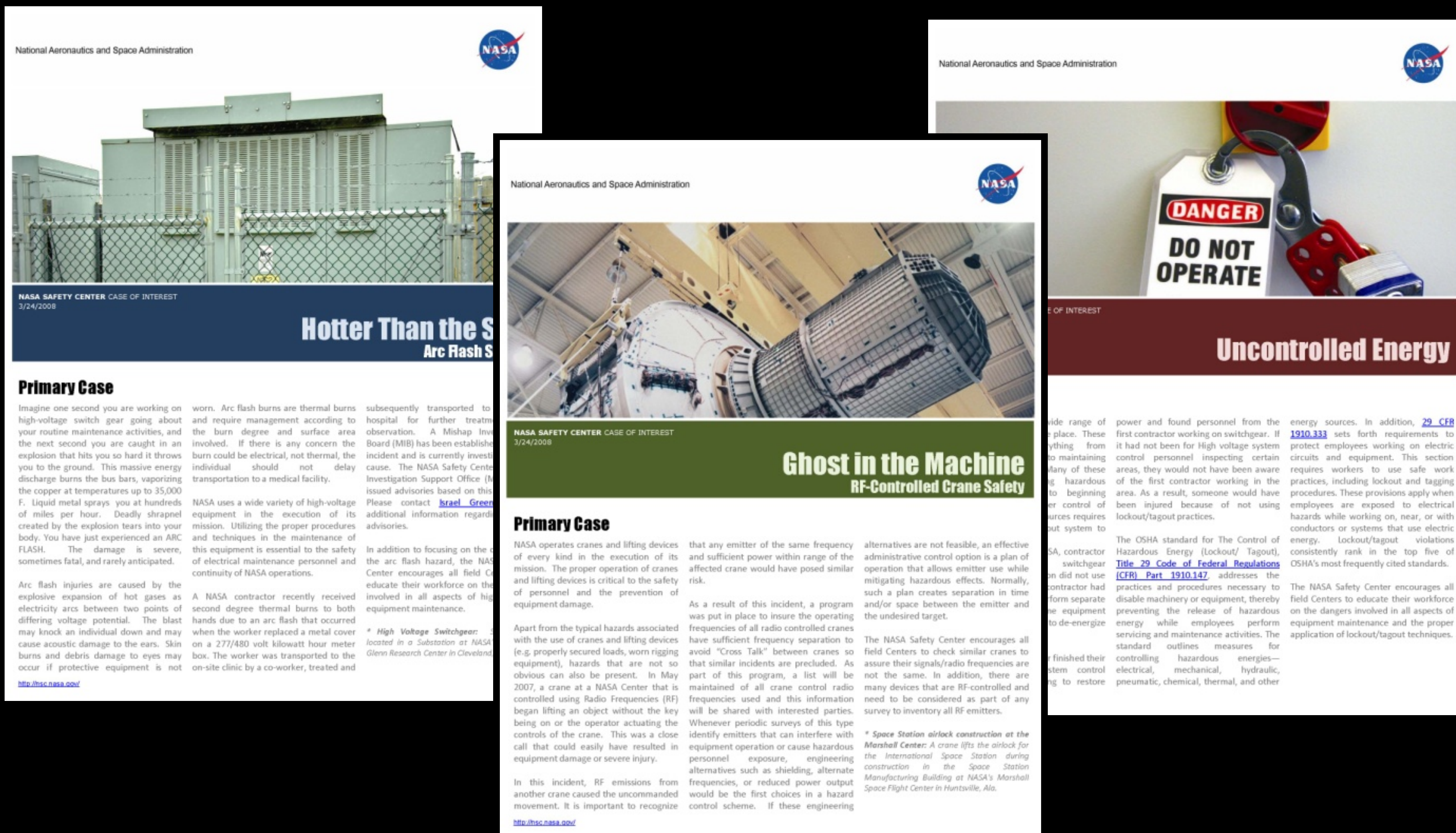
COI knowledge sharing product

- Selection considerations for the desired message
  - Agency goals
  - Trends for safety awareness
  - Applicability to general operations
  - Timeliness of information
  - Relevance to developing programs
  - Relevance to recent mishaps
  - Recent audit findings
  - Applicability to current agency business processes

COI History

- **Cases of Interest “concept of operations”**
- **Began in 2006**
- **Produced monthly from the prevention marker analysis of mishaps, close calls and hazards reported into the *Incident Reporting Information System (IRIS)***
- **Representing cases which typifies a specific mishap trend or have broad based applicability to both ground and flight operations**
- **2 - 4 page write-up complimented by web site with links to related information such as similar incidents, related requirements, best practices, highlights from the event, applicable training, and suggested auditing and quality control**
- **Key Points**
  - Background and overview of failure
  - Compliance information, related documentation and other background data that can assist members of the NASA Community in mitigating the hazards associated with the CoI event.
  - Applicability to NASA operations

Sample COI Knowledge Sharing Product



National Aeronautics and Space Administration

NASA SAFETY CENTER CASE OF INTEREST
3/24/2008

Hotter Than the S...
Arc Flash S...

National Aeronautics and Space Administration

Uncontrolled Energy

National Aeronautics and Space Administration

NASA SAFETY CENTER CASE OF INTEREST
3/24/2008

Ghost in the Machine
RF-Controlled Crane Safety

Primary Case

NASA operates cranes and lifting devices of every kind in the execution of its mission. The proper operation of cranes and lifting devices is critical to the safety of personnel and the prevention of equipment damage.

Apart from the typical hazards associated with the use of cranes and lifting devices (e.g. properly secured loads, worn rigging equipment), hazards that are not so obvious can also be present. In May 2007, a crane at a NASA Center that is controlled using Radio Frequencies (RF) began lifting an object without the key being on or the operator actuating the controls of the crane. This was a close call that could easily have resulted in equipment damage or severe injury.

In this incident, RF emissions from another crane caused the uncommanded movement. It is important to recognize that any emitter of the same frequency and sufficient power within range of the affected crane would have posed similar risk.

As a result of this incident, a program was put in place to insure the operating frequencies of all radio controlled cranes have sufficient frequency separation to avoid "Cross Talk" between cranes so that similar incidents are precluded. As part of this program, a list will be maintained of all crane control radio frequencies used and this information will be shared with interested parties. Whenever periodic surveys of this type identify emitters that can interfere with equipment operation or cause hazardous personnel exposure, engineering alternatives such as shielding, alternate frequencies, or reduced power output would be the first choices in a hazard control scheme. If these engineering alternatives are not feasible, an effective administrative control option is a plan of operation that allows emitter use while mitigating hazardous effects. Normally, such a plan creates separation in time and/or space between the emitter and the undesired target.

The NASA Safety Center encourages all field Centers to check similar cranes to assure their signals/radio frequencies are not the same. In addition, there are many devices that are RF-controlled and need to be considered as part of any survey to inventory all RF emitters.

** **Space Station airlock construction at the Marshall Center:** A crane lifts the airlock for the International Space Station during construction in the Space Station Manufacturing Building at NASA's Marshall Space Flight Center in Huntsville, Ala.*

http://nsc.nasa.gov/

NASA SAFETY CENTER

Using the knowledge sharing product

What YOU can do…

- Identify where to infuse the corrective and preventative actions into current processes to mitigate or eliminate those precursors and hazards identified in the CoI
- Identify personnel that would be integrators, implementers and disseminators of this information or adjust expertise required to address current and potential hazards
- Expedite communication on these precursors and hazards to your team

Read it and recognize the hazard or risk

Make relevant personnel aware

Perform preventative action

CoI Review promotes Mission success

What this will do for your team…

- Provides a basis for a broader discussion of precursors and hazards related to a particular topic
- Assists identification of “gaps” in current requirements, contracts/contract processes, training, operational processes
- Facilitates timely hazard identification and safety awareness and development of effective countermeasures

COI - Where to find….

- The CoI is posted on the NSC website: (http://nasa.nsc.gov)
- The CoI provides links to relevant areas of the NSC website and or other agency websites
- Electronic distribution of PDF versions

Case of Interest PBMA workgroup

Additional information can be found by joining the PBMA CoI working group.

IRIS #	Date	Site	Classification	Description
2008-042-00009	2/8/2008 11:50	JPL	Type D	JPL#1598 - Power outage of entire MSSCC complex.

Detailed Description	Amplifying Information, Analyst Questions
See attached "Accident Notification Form." Note: 2008-039-00007 was a duplicate entry and has been deleted.	A worker of the "UTE Complejo Especial" was working on a high voltage panel. When he tried to connect to ground a high voltage conductor, it flared. When standing back he slightly banged his head. Worker had hard hat, electrical face shield, electrical gloves and insulating rug. Several electrical components of the panel burned (transformers, coils, etc).

Severity	Likely	Complex	Coupled	Control Failure	Latent Condition	Doc	CAP
Injury	Yes	No	No	1.1 Unidentified hazard	Energized circuit	No	No

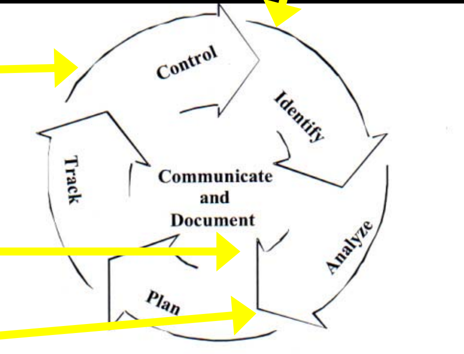
Av/Op S&MA	Quality Eng	R&M	Software Safety	Systems Safety
Yes	Maybe-insufficient cause data	Yes	No	Yes

Latent Condition!

Failed Control!

Broad Effects!

Catastrophic Outcome!



Summary

- There are great case study resources out there to help create stronger project teams
  - Insight
  - Communication
  - Teambuilding

- The ball is now in your court to take advantage of these resources and plan to use them

- Contact: nasa-nsc@nasa.gov